PATENT ABSTRACTS OF JAPAN

(11)Publication number : **2003-303175**
(43)Date of publication of application : **24.10.2003**

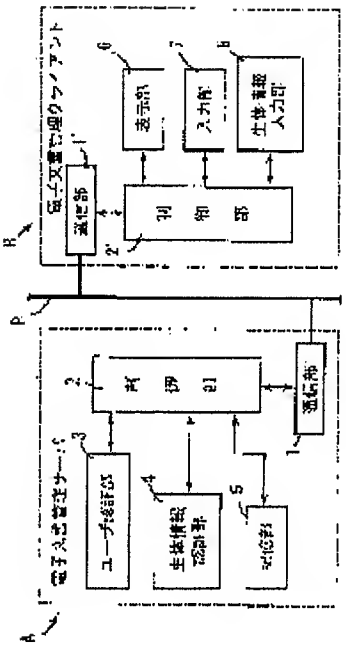
(51)Int.Cl. **G06F 15/00**
G06F 12/00

(21)Application number : **2002-109195**
(22)Date of filing : **11.04.2002**

(71)Applicant : **RICOH CO LTD**
(72)Inventor : **SHIMA MASAKAZU**

(54) ELECTRONIC DOCUMENT MANAGING SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide an electronic document managing system capable of keeping high security accuracy by allowing selection of an input form of authenticated information in response to an importance level in security in the inputted authenticated information.
SOLUTION: One of authenticating methods of authentication in the case of using only authenticated information such as a password or an ID card having a relatively high possibility of a spoofing behavior by others and authentication in the case of using organism information such as a finger-point, a voice print, and a retina pattern can be selected by a user. The managing system has a means 2 capable of classifying an access right to a document when each authenticating method is selected.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2003－303175
（P2003－303175A）
(43)公開日　平成15年10月24日(2003.10.24)

(51)Int.Cl.⁷	識別記号	FI	テーマコード(参考)
G06F 15/00	330	G06F 15/00	330D 5B082
			330B 5B085
12/00	537	12/00	537A

審査請求　未請求　請求項の数3　ＯＬ　（全７頁）

(21)出願番号　特願2002－109195(P2002－109195)

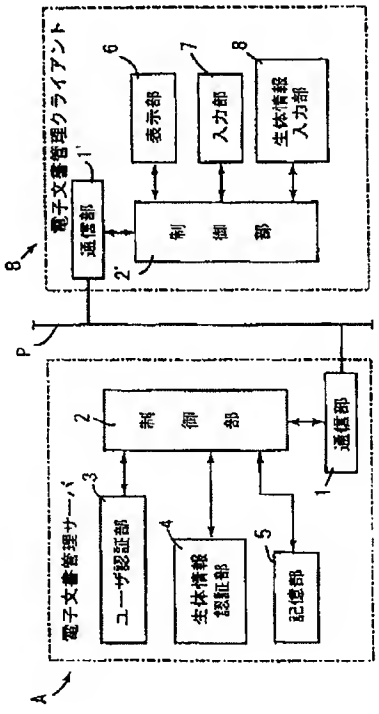
(22)出願日　平成14年４月11日(2002.4.11)

(71)出願人　000006747
株式会社リコー
東京都大田区中馬込１丁目３番６号
(72)発明者　志摩　昌和
東京都大田区中馬込１丁目３番６号・株式会社リコー内
(74)代理人　100067873
弁理士　樺山　亨　（外１名）

Ｆターム(参考)　5B082 EA12
5B085 AA08 AE03 AE06 AE12 AE25

(54)【発明の名称】　電子文書管理システム

(57)【要約】
【課題】　入力される認証情報においてセキュリティ上での重要度に応じて認証情報の入力形態を選択できるようにして高度なセキュリティ精度を維持できるようにすることができる電子文書管理システムを提供する。
【解決手段】　パスワードやＩＤカードといった、他人が成りすまし行為をする可能性が比較的高いと考えられる認証情報のみを利用した場合の認証と、指紋・声紋・網膜パターンなどの生体情報を利用した場合の認証といういずれかの認証方法がユーザから選択可能であり、各認証方法が選択された場合の文書へのアクセス権を区別する事が可能な手段２を備えたことを特徴する。



【特許請求の範囲】
【請求項１】パスワードやＩＤカードといった、他人が成りすまし行為をする可能性が比較的高いと考えられる認証情報のみを利用した場合の認証と、指紋・声紋・網膜パターンなどの生体情報を利用した場合の認証といういずれかの認証方法がユーザから選択可能であり，各認証方法が選択された場合の文書へのアクセス権を区別する事が可能な手段を備えたことを特徴とする電子文書管理システム。
【請求項２】パスワードやＩＤカードといった、他人が成りすまし行為をする可能性が比較的高いと考えられる認証情報のみを利用した場合の認証と、加えて指紋・声紋・網膜パターンなどの生体情報も利用した場合の認証といういずれかの認証方法がユーザから選択可能であり，各認証方法が選択された場合の文書へのアクセス権を区別する手段を備えたことを特徴とする電子文書管理システム。
【請求項３】請求項１または２記載の電子文書管理システムにおいて、
文書へのアクセス権を、認証されたユーザ毎に区別することが可能な手段を備えたことを特徴とする電子文書管理システム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、電子文書管理システムに関し、特に、特定ユーザと一般ユーザとが参照する際の認証処理に関する。
【０００２】
【従来の技術】近年、通信回線を利用した文書閲覧サービスあるいは金融機関での出納処理サービスなどが多用されるようになってきており、この場合には、サービスを受けようとするユーザの認証が必要とされている。ユーザ自身であることの認証方法として一般的なのは、パスワードやＩＤカードなどの入力を要求する方法があり、この方法では、それら入力情報が予め登録されているユーザ情報と適合した場合に認証が成功したと判断するようになっている。しかし、パスワードやＩＤカードは偽造が可能であったり漏洩する虞があることで保全性（セキュリティ機能）が低く、これにより不正アクセスとの識別ができないことがある。
【０００３】ユーザ自身の認証に際しての不正アクセスを防止する認証方式として、ユーザの指紋・声紋・網膜データ等の生体情報を利用する方法がある（例えば、特開２０００－２５９２７８号公報）。この方法は、指紋や目の虹彩、声紋あるいは網膜血管分布（網膜パターン）などを予め認証部において登録しておき、入力された生体情報と比較するようになっている。また、上記公報では、生体情報の再現性が悪い場合の誤判断を防止することを考慮して、上述したパスワードやＩＤ情報などを補助情報として要求し、両者の情報に基づく衝合結果を合わせて最終的な認証結果を得るようにした構成が開示されている。これにより、両者の情報を併せることで保全性（セキュリティ性能）が高められることになる。
【０００４】
【発明が解決しようとする課題】生体情報を適用する場合には、入力対象となる各種データの登録設定に次のような問題が生じる。アクセスする際に必ず生体情報による認証を要求すると、システムを利用するユーザ全員の生体情報を登録・管理する必要があり、例えば「一般職に所属するユーザは一つのグループとして扱い、文書に対する権限を統一したい」といった場合でも一般職に所属するユーザ全員の生体情報をメンテナンスしなければならない等といった不便が生じる。つまり、偽造や漏洩情報が用いられやすい認証情報に加えて生体情報も同時に入力することによりセキュリティ精度を上げるような場合には、両者の認証情報の照合が必要となり、照合に要する時間、コストがきわめて大きくなる。また、「社外からのお客様はＧｕｅｓｔアカウントを利用して頂いて特定の文書だけを参照して頂くようにしたい」といった場合においても，Ｇｕｅｓｔアカウントとしてどのような生体情報を記録しておけば良いのかあるいは、その記録した情報の検索（照合）条件をどのようにするかなどの問題が生じる。このように、セキュリティ精度の向上を図る際には、入力された認証情報に基づく検索および照合時間が多大となる虞がある。しかも、生体情報のみの入力あるいはパスワードやＩＤカードを用いた情報のみを用いた入力に関する頻度が一様でないことからセキュリティ機能の精度設定によってはシステムコストが多大なものとなる虞もある。
【０００５】本発明の目的は、第１に、入力される認証情報においてセキュリティ上での重要度に応じて認証情報の入力形態を選択できるようにして高度なセキュリティ精度を維持できるようにすることができる電子文書管理システムを提供することにある。
【０００６】第２の目的としては、高度なセキュリティ精度が要求される文書へのアクセス権を要求する認証情報の入力がある場合において確実にセキュリティ精度を維持して認証情報の照合が行える電子文書管理システムを提供することにある。
【０００７】第３の目的は、文書尾へのアクセス権を、認証されたユーザ毎に区別することにより、よりきめ細やかなアクセス権を設定してセキュリティ精度を維持できる電子文書管理システムを提供することにある。
【０００８】
【課題を解決するための手段】請求項１記載の発明は、パスワードやＩＤカードといった、他人が成りすまし行為をする可能性が比較的高いと考えられる認証情報のみを利用した場合の認証と、指紋・声紋・網膜パターンなどの生体情報を利用した場合の認証といういずれかの認証方法がユーザから選択可能であり、各認証方法が選択

された場合の文書へのアクセス権を区別する事が可能な手段を備えたことを特徴としている。

【０００９】請求項２記載の発明は、パスワードやＩＤカードといった、他人が成りすまし行為をする可能性が比較的高いと考えられる認証情報のみを利用した場合の認証と、加えて指紋・声紋・網膜パターンなどの生体情報も利用した場合の認証といういずれかの認証方法がユーザから選択可能であり、各認証方法が選択された場合の文書へのアクセス権を区別する手段を備えたことを特徴としている。

【００１０】請求項３記載の発明は、請求項１または２記載の電子文書管理システムにおいて、文書へのアクセス権を、認証されたユーザ毎に区別することが可能な手段を備えたことを特徴としている。

【００１１】

【発明の実施の形態】以下、図面により本発明の実施の形態を説明する。図１は、本発明の実施形態による電子文書管理システムを構成するシステム構成図である。同図において、電子文書管理システムは、通信回線Ｐ（ネットワーク）を介して電子文書管理サーバＡと、通信回線Ｐを介して電子文書管理サーバＡにアクセスするためのユーザ側での操作が可能な電子文書管理クライアント部分Ｂとで構成されている。電子文書管理サーバＡには、通信回線Ｐを介してクライアントからの認証要求や文書参照要求を受けて処理するとともに制御部２との間でこれら要求および要求に対する結果をクライアント側に出力する部分である。

【００１２】通信部１に接続されている制御部２には、ユーザ認証部３，生体情報認証部４，記憶部５が接続されており、制御部２は、文書情報やアクセス権リストが格納されている記憶部５から保存されている文書情報を取得して通信部１に渡したり、逆に通信回線Ｐから送られてきた電子文書クライアント部Ｂからの認証要求や文書参照要求を受けて処理する実行部として機能する手段を構成している。

【００１３】制御部２は、パスワードやＩＤカードといった他人がなりすまし行為をする可能性が高いと考え得る認証情報のみを利用した場合の認証と、指紋・声紋お呼びもうまくパターンなどの生体情報を利用した場合あるいは生体情報を合わせて利用した場合とがユーザにおいて選択された場合のいずれにも対処して、ユーザからの要求内容に対するアクセス権を決定するという区別処理ができる手段として構成されている。

【００１４】電子文書管理クライアントＢには、電子文書管理サーバＡに設けられているものと同様な通信部１’と制御Ｐ部２’とが備えられている。制御部２’は、通信部１’へ送られてきた文書情報を表示部へ渡したり、逆に入力部や生体情報入力部から入力されたユーザＩＤ，パスワード，生体情報などの各種情報を通信部へ渡す部分として機能する手段を構成している。表示部６は、文書などを表示する部分であり、通信部１’は、通信回線Ｐ（ネットワーク）を通じて電子文書管理サーバＡと情報を授受する部分であり、入力部７は、ユーザＩＤやパスワード等を入力する部分として用いられ、生体情報入力部８は、生体情報の入力を行う部分である。入力部７では、電子文書管理サーバＡ側に保存されている文書の検索データを入力することができ、生体情報入力部８では、指紋・声紋・網膜パターン等を入力できる検知部が設けられている。

【００１５】本実施形態では、図１に示した構成において、図２に示すような作業指令系統が構成される。図２において、制御部（便宜上、符号１０で示す）では、通信部（便宜上、符号１１で示す）を介してユーザからの要求がある場合、ユーザの認証をユーザ認証部（便宜上、符号１２で示す）および生体情報認証部（便宜上、符号１３で示す）のいずれか若しくは両方を選択することにより行い、その結果に応じて記憶部（便宜上、符号１４で示す）から要求された文書のアクセス権に基づく文書情報を通信部１を介してユーザに提示する。この場合、後で説明するが、認証方式をユーザが選択することができるようになっている。記憶部１４における文書テーブル１４Ａには、表１に示すように、文書を一意に識別するための識別コードである文書ＩＤおよびこれに対応する文書名が関係づけされて登録されている。

【００１６】

【表１】

文書ＩＤ	文書名
０００１	人事情報
０００２	設計書
０００３	会社案内

【００１７】表１では、一例として、会社内で用いられる文書が対象となっている。

【００１８】記憶部１４におけるアクセス権テーブル１４Ｂには、表２に示すように、文書管理システム内でアクセス権を一意に識別するＩＤ（以下ではアクセス権ＩＤ）を含んだ、アクセス権に関する情報が関係づけられて登録されている。

【００１９】

【表２】

アクセス権ＩＤ	文書ＩＤ	アカウント	アクセス権	
			生体情報認証なし	生体情報認証有り
0001	0001	userA	アクセス不可	参照権
0002	0001	一般	アクセス不可	アクセス不可
0003	0001	Guest	アクセス不可	アクセス不可
0001	0002	userA	参照権	参照権、更新権
0001	0002	一般	参照権	参照権
0001	0002	Guest	アクセス不可	アクセス不可
0001	0003	一般	参照権	参照権、更新権
0001	0003	Guest	参照権	参照権

【００２０】表２は、表１に示した文書ＩＤを前提として設定されている。

【００２１】ユーザ認証部１２におけるユーザ情報テーブル１２Ａには、表３に示すように、ユーザＩＤとパスワードおよびそのユーザの所属階級といったユーザに関する情報（アカウント情報）とが関係づけて登録されている。

【００２２】

【表３】

ユーザＩＤ	所属階級	パスワード
userA	管理	*****
userB	一般	********
Guest	社外	

【００２３】生体情報認証部１３における生体情報テーブル１３Ａには，ユーザＩＤとそのユーザの生体情報データとが関係づけて登録されている。

【００２４】

【表４】

ユーザＩＤ	生体情報データ
userA	〈userAの生体情報データ〉
userB	〈userBの生体情報データ〉

【００２５】表４に示す生体情報テーブル１３Ａには、上述した指紋・声紋・網膜パターンの全てが登録されている。

【００２６】図１に示した電子文書クライアント部Ｂにおける入力部７では、図３に示すようなダイアログ表示（便宜上、図３中、符号７Ａ、７Ｂにより選択キーを示す）が行われ、ユーザによる生体情報を利用した認証方式かどうかを決定するようになっている。認証処理は次の手順により実行される。

（１）ユーザからユーザＩＤおよびパスワードを入力されると、ユーザ情報テーブル１２Ａを利用して照合する。

（２）（１）において照合が成立し、いわゆる、照合に成功し、かつ、ユーザが生体情報認証を行うことを指定した場合には、ユーザからの生体情報テーブル１３Ａを利用して照合処理を行う。

（３）（１）において照合に成功した時点でユーザが生体情報認証を行わないことを指定（選択）した場合には、ユーザ情報テーブル１２Ａから取得される所属情報をセッション情報として保持し、認証処理を終える。

（４）（２）において照合に成功した場合には、ユーザ情報テーブル１２Ａから取得される所属情報と、生体情報認証処理において照合が成功しているという情報を合わせてセッション情報として保持し、認証処理を終える。

【００２７】本実施形態は以上のような構成を用いて制御部において図４に示す処理が実行される。図４は、上記（１）～（４）に挙げた手順を示すフローチャートであり、ユーザＩＤおよびパスワードが入力されると（ＳＴ１）、照合処理が行われる（ＳＴ２）。照合処理では、入力された情報に基づき、表３に示したテーブルを用いてユーザのアカウント情報が識別され、照合が成功したかどうかが判別される（ＳＴ３）。照合が失敗した場合には、エラー処理が行われ（ＳＴ４）、この処理では、表示部６に入力情報が間違っている旨の表示などが行われる。

【００２８】アカウント情報に関する照合が成功した場合には、生体情報が入力されたかどうか、つまり、ユーザによる生体情報の認証情報の照合が選択されたかどうかを、この情報を利用するかどうかにより判別される（ＳＴ５）。生体情報の入力がある場合（ＳＴ６）には、表４に示したテーブルを用いて照合処理が行われ（ＳＴ７）、照合が成功したかどうかが判別される（ＳＴ８）。

【００２９】生体情報を用いた照合が成功した場合には、その情報内容をセッション情報として追加（保持）し（ＳＴ９）、所属情報をセッションに追加（保持）する（ＳＴ１０）。

【００３０】上述した手順では、パスワードおよびＩＤ情報を入力した場合の照合に加えて、生体情報が入力された場合を併せて認証のための処理に用いるだけでなく、ユーザの選択によりパスワードおよびＩＤ情報のみが用いられた場合においても認証内容をセッション情報に追加することができるので、パスワードとＩＤ情報を入力することによりアクセス権を取得する場合と上記情報に加えて生体情報を合わせて入力することによりアクセス権を得する場合とをユーザの選択に応じて実行できるようになっている。

【００３１】ユーザによる認証情報の照合形態の選択は、アクセス権を得ようとする対象となる文書内容のセキュリティに依存しており、高度なセキュリティを必要

とする必要のない文書へのアクセス権を得ようとする場合には、パスワードやＩＤ情報のみによりアクセス権を得ることができる。従って、高度のセキュリティを必要とする場合には、偽造や漏洩の虞があるパスワードやＩＤのみではなく、ユーザの生体情報を認証情報として要求することにより高度なセキュリティを維持した状態でのアクセス権を得るようにすることができる。このように、ユーザの認証情報の照合形態を選択することにより、高度なセキュリティを維持する必要がないに文書へのアクセス権が要求された場合の照合に要する時間を短縮することができる。

【００３２】図５は、図４に示した各種入力情報に基づく電子文書クライアント部Ｂからの要求内容に対応して、アクセス権の決定を行う処理を示すフローチャートであり、同図において、セッション情報が追加されると（ＳＴ１１）、表２に示したアクセス権に関するテーブルを用いてアクセス権の決定が実行される（ＳＴ１２）。このステップでは、ユーザからの文書へのアクセスがあった場合に、セッション情報と文書テーブル（表１参照）および表２に示すアクセス権に関するテーブルを参照してアクセスの許可あるいは拒否が決定される。

【００３３】アクセス権の決定において許可された場合には、要求されている文書を検索し、検索結果を表示部６に表示する（ＳＴ１３）。

【００３４】ステップＳＴ１２でのアクセス権の決定に際しては、表１乃至４からも明らかなように、例えば、表２に示すように、ユーザＡ（ｕｓｅｒＡ）が文書データのうちの「人事情報」（表１参照）の参照を要求した場合、指紋認証を行っていれば文書へのアクセス権が許可されるが、指紋認証を行っていない場合にはアクセス権が拒否される。また、表２において、ユーザＢ（ｕｓｅｒＢ）が文書「会社案内」（表１参照）の更新を要求したような場合、もし指紋認証を行っていればアクセス権は許可される。つまり、ユーザＢは組織「一般」に所属しているので、指紋認証が行われることによりアクセス権が許可され、指紋認証が行われていない場合にはアクセス権が拒否される。このように、アクセス権を得るための照合によって認証されたユーザ毎に区別することができるので、アクセス権を要求したユーザに対してアクセス権の照合条件を細分化していくことができる。

【００３５】なお、本発明は、上記したような実施の形態と同様に、サーバとクライアントとを備えたシステム構成を前提とする場合には、認証情報を上述した例に限らないこと勿論可能である。しかも、ユーザ認証部や生体情報認証部はサーバから独立していてもよく、クライアントとサーバとは一体であっても良い。この場合には通信部が不要となる。

【００３６】

【発明の効果】請求項１記載の発明によれば、パスワードやＩＤカードといった，他人が成りすまし行為をする可能性が比較的高いと考えられる認証情報のみを利用した場合の認証と、指紋・声紋・網膜パターンなどの生体情報を利用した場合の認証といういずれかの認証方法をユーザから選択可能とすることができるので、高度なセキュリティを必要とする場合とさほどでない場合とをユーザの認証情報入力形態により設定することができ、仮に高度なセキュリティが要求されるような場合と区別することが可能となり、常時高度なセキュリティを必要とする場合のような照合時間をかける必要をなくして照合時間の短縮化による使い勝手の良さを得ることが可能となる。

【００３７】請求項２記載の発明によれば、認証情報の照合方式を選択可能な場合であっても、高度なセキュリティが要求される場合には、偽造や漏洩が可能な場合があるパスワードやＩＤカード等の認証情報に加えて、指紋・声紋・網膜パターンなどの生体情報も強制的に照合できるようにすることにより、既存のパスワードやＩＤカードによる認証システムが導入されている電子文書管理システムを対象とした場合のセキュリティ機能を確保することが可能となる。

【００３８】請求項３記載の発明によれば、文書に対するアクセス権を，認証されたユーザ毎に区別することにより，セキュリティを維持しながら、よりきめ細やかなアクセス権設定が可能となる。

【図面の簡単な説明】

【図１】本発明の実施形態による電子文書管理システムの構成図である。

【図２】図１に示した電子文書管理システムに用いられるユーザ認証部の構成を説明するためのブロック図である。

【図３】認証情報の照合形態を選択する入力部を説明するための図である。

【図４】図１に示した電子文書管理システムの作用を説明するためのフローチャートである。

【図５】図４に示した電子文書管理システムにおけるアクセス権の決定のための処理を説明するためのフローチャートである。

【符号の説明】

Ａ　電子文書管理サーバ

Ｂ　電子文書管理クライアント

１，１’　通信部

２，２’　文書へのアクセス権を決定する手段をなす制御部

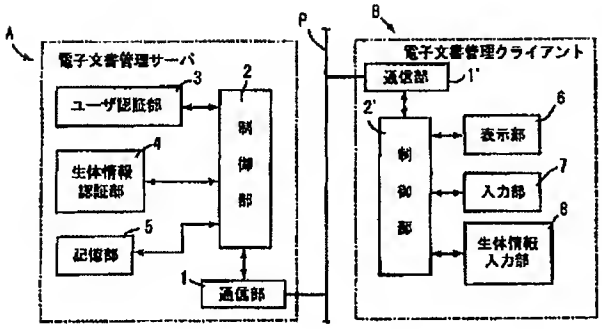
３　ユーザ認証部

４　生体情報認証部

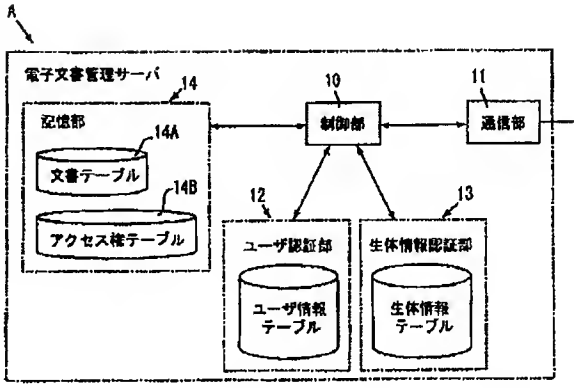
７　入力部

７Ａ、７Ｂ　認証方式を選択するダイアログ表示部

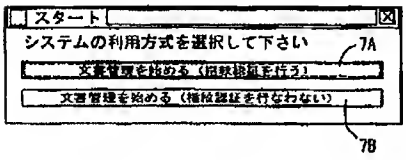
【図１】


A
電子文書管理サーバ
ユーザ認証部
3
2
制御部
生体情報認証部
4
5
記憶部
1
通信部
P
B
電子文書管理クライアント
通信部
1'
2'
制御部
表示部
6
入力部
7
生体情報入力部
8

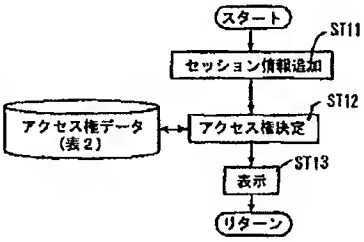
【図２】


A
電子文書管理サーバ
14
記憶部
14A
文書テーブル
14B
アクセス権テーブル
10
制御部
11
通信部
12
ユーザ認証部
ユーザ情報テーブル
13
生体情報認証部
生体情報テーブル

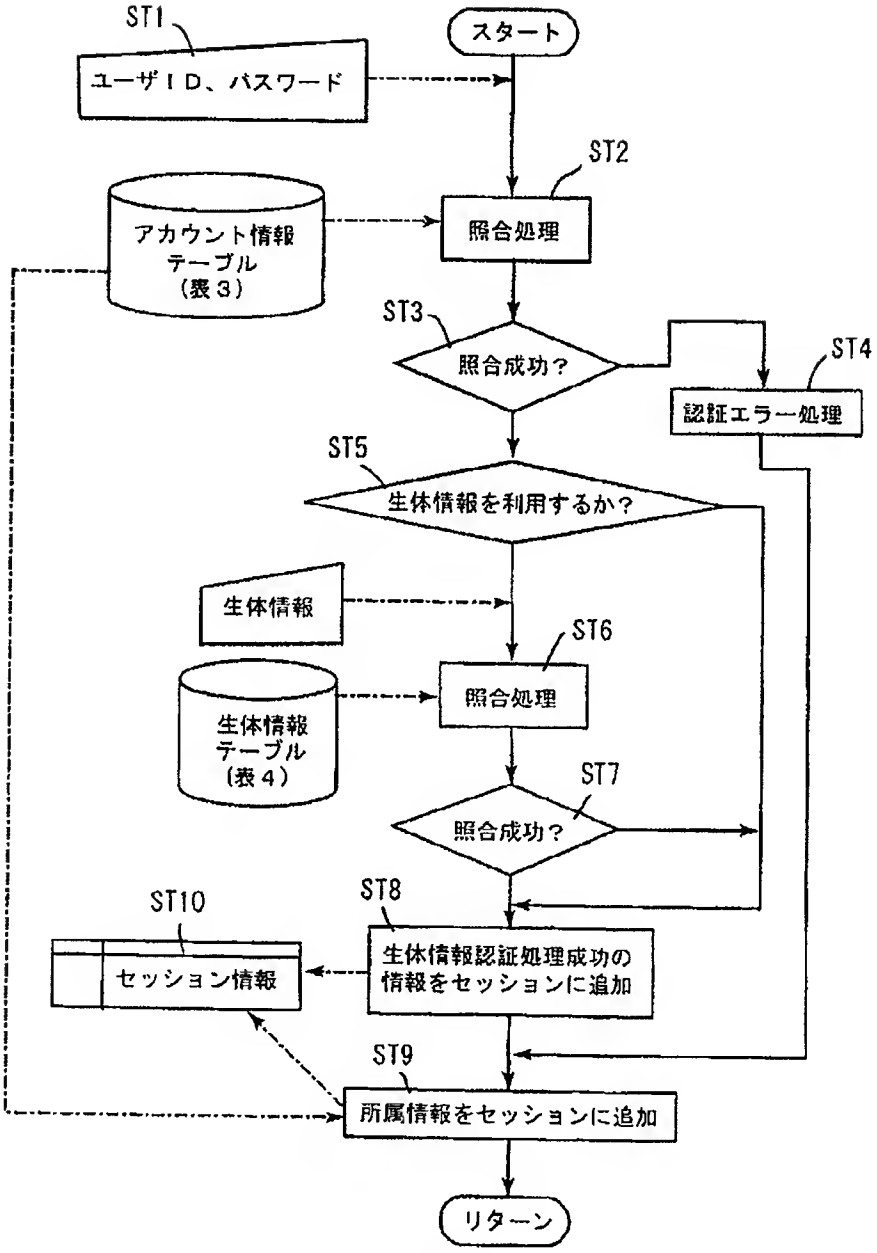
【図３】


スタート
システムの利用方式を選択して下さい
7A
文書管理を始める（指紋認証を行う）
文書管理を始める（権限認証を行なわない）
7B

【図５】


スタート
ST11
セッション情報追加
ST12
アクセス権データ（表２）
アクセス権決定
ST13
表示
リターン

【図4】


ST1
ユーザＩＤ、パスワード
スタート
ST2
アカウント情報
テーブル
（表３）
照合処理
ST3
照合成功？
ST4
認証エラー処理
ST5
生体情報を利用するか？
生体情報
ST6
照合処理
生体情報
テーブル
（表４）
ST7
照合成功？
ST10
ST8
セッション情報
生体情報認証処理成功の
情報をセッションに追加
ST9
所属情報をセッションに追加
リターン